Visuelle Kryptografie

Proseminar:
Moderne kryptografische Verfahren

Dozent:
Prof. Johannes Köbler

Autor:
Andreas Schreiber

Datum:
14.02.2002

Inhalt:

INHALT: **2**

1. ÜBERBLICK: **3**

2. GRUNDLEGENDES MODELL: **3**

2.1 Wahl der Parameter: 4
2.2 Allgemein gilt für eine Lösung eines *k* aus *n*-Schemas: 4
2.3 Matrizen für ein 2 aus 2-Schema: 5
2.4 Ähnlichkeiten zum One-Time-Pad: 6
2.5 Entschlüsseln: 6

3. LÖSUNGEN FÜR KLEINE *N* UND *K*: **7**

3.1 Das 2 aus *n*-Schema: 7
3.2 Das 3 aus 3-Schema: 7

4. DAS *N* AUS *N*-SCHEMA: **8**

5. DAS *K* AUS *N*-SCHEMA: **9**

6. ERWEITERUNGEN: **9**

7. ZUSAMMENFASSUNG: **10**

8. LITERATUR UND LINKS: **11**

1. Überblick:

- Zum ersten Mal veröffentlicht 1994 auf der *EUROCRYPT ´94* (09. – 12. Mai) in Perugia, Italien. Entwickelt von Moni Naor und Adi Shamir.

- Das System ist sehr simpel in der Anwendung und bedarf keiner besonderen Berechnung durch Hardware oder Personen mit besonderem Wissen über Kryptografie. Schlüssel und geheime Botschaft können z. B. per Fax, E-Mail oder der Post verschickt werden. Die geheime Botschaft kann allein durch den Einsatz des menschlichen Auges entschlüsselt werden (visuelles Verschlüsselungsschema: **V**isual **C**ryptography **S**cheme, **VCS**).

- Grundprinzip: Eine geheime Botschaft wird in Bildpunkte aufgeteilt. Die einzelnen Bildpunkte werden in weitere Unterpunkte aufgeteilt, welche per Zufall ausgewählt entweder schwarz oder weiß eingefärbt werden. Es entsteht auf jeder Folie ein Muster, welches nicht mehr von Rauschen zu unterscheiden ist. Diese Folien können an verschiedene Teilnehmer verteilt werden (*Secret Sharing*; Adi Shamir, 1979).
  Zum Entschlüsseln der geheimen Botschaft müssen nur die einzelnen Folien übereinander gelegt werden. Die geheime Botschaft wird dann sichtbar.

- Das Verfahren ist absolut sicher, da für jeden Unterpunkt eines Bildpunktes einzeln per Zufall entschieden wird, ob er schwarz oder weiß ist.

- Bei Erweiterung auf ein *k* aus *n*-Schema gilt: Nur wenn eine Mindestanzahl *k* Personen von einer Gesamtzahl *n* von Teilnehmern zusammen arbeiten, kann die Originalbotschaft wieder hergestellt werden. Bei weniger Personen kann die geheime Botschaft nicht entschlüsselt werden.

2. Grundlegendes Modell:

Das ursprüngliche Modell kann wie folgt beschrieben werden:
Die zu verschlüsselnde, geheime Botschaft wird in rechteckige Bildpunkte (Bildelemente, Pixel) unterteilt (gerastert). Ein Bildpunkt enthält je zwei Unterpunkte. Diese sollten so dicht beieinander liegen, dass das menschliche Auge sie als einzelne Bildpunkte wahrnimmt. Jedem Unterpunkt wird nun zufällig die Farbe Schwarz oder Weiß (oder besser: transparent) zugeordnet. Für einen Bildpunkt gibt es zwei verschiedenen Möglichkeiten, seine beiden Unterpunkte durch eine Kombination von Schwarz und Weiß darzustellen. Ist der Punkt weiß, bekommen beide Unterpunkte die gleiche Verteilung von Schwarz und Weiß (transparent). Bei einem schwarzen Punkt haben beide Unterpunkte eine komplementäre Verteilung von Schwarz und Weiß (transparent). Die Menge der Unterpunkte eines Bildpunktes nennt man *Share*.

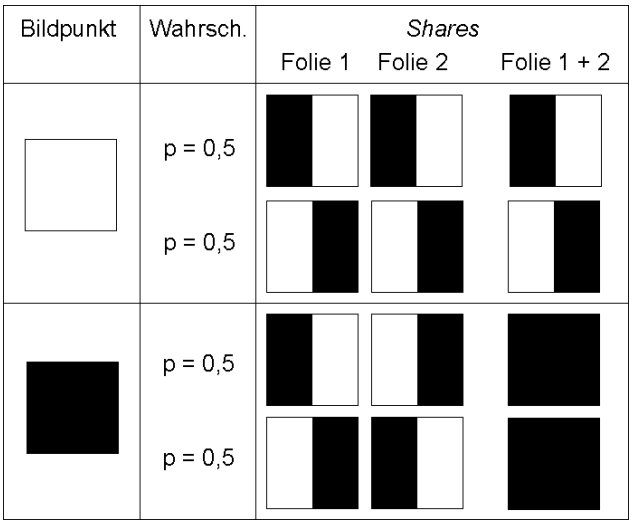

Abbildung 1: Bildung der Grauwerte.

Dies kann durch eine $n \times m$-Matrix $S = [s_{ij}]$ dargestellt werden, wobei $s_{ij} = 1$ gdw. der j-te Unterpunkt des i-ten *Shares* schwarz ist und $s_{ij} = 0$ gdw. der j-te Unterpunkt des i-ten *Shares* weiß ist. Die einzelnen Zeilen der Matrix entsprechen den *Shares* der Teilnehmer. Legt man nun die Folien $1 \ldots n$ über einander, so erhält man die ODER-Verknüpfung aller *Shares* (also der Zeilen der Matrix S). Der resultierende Grauwert entspricht dem Hamminggewicht $H(V)$ des Vektors V. Der Grauwert eines Bildpunktes wird als weiß wahrgenommen falls $H(V) \leq d - \alpha * m$, und als schwarz, falls $H(V) \geq d$ mit $d = 1 \ldots m$ und einer relativen Differenz $\alpha > 0$.

2.1 Wahl der Parameter:

Die Matrix S_0, welche für die weißen Bildpunkte benutzt wird, stammt aus einer Menge C_0. Die Matrix S_1 für die schwarzen Bildpunkte aus einer Menge C_1. Die ausgewählte Matrix legt die m Bildpunkte jedes der n *Shares* fest.
Die Größe der Mengen C_0 und C_1 ist r. Die Anzahl der Zufallsbits, die man benötigt, um eine Matrix aus C_0 oder C_1 auszuwählen ist $\log r$. Sie hat keinen Einfluss auf die Qualität des entstehenden Bildes.
Die Anzahl der Unterpunkte m in einem *Share* sollte möglichst klein gewählt werden, wo hingegen der relativer Gewichtsunterschied zwischen entschlüsseltem schwarzen und weißen Bildpunkt α relativ groß sein sollte.
Die Anzahl der Folien n, auf die die geheime Botschaft verteilt wird (Anzahl der Teilnehmer am *Secret Sharing*) und die Anzahl der nötigen Folien k, um die geheime Botschaft zu entschlüsseln können dagegen den Gegebenheiten nach belieben angepasst werden.

2.2 Allgemein gilt für eine Lösung eines *k* aus *n*-Schemas:

1. $\forall S_0 \in C_0$ gilt: $H(V) \leq d - \alpha * m$ wird von jedem V von beliebigen k der n Zeilen von S erfüllt.
2. $\forall S_1 \in C_1$ gilt: $H(V) \geq d$ wird von jedem V von beliebigen k der n Zeilen von S erfüllt.
3. $\forall$Teilmengen $\{i_1 \ldots i_q\}$ von $\{1 \ldots n\}$ mit $q < k$ seinen D_0 und D_1 die Mengen von Matrizen, die man bei Beschränkung der Mengen C_0 und C_1 auf die Zeilen

$\{i_1 \ldots i_q\}$ erhält. D_0 und D_1 enthalten dann die gleichen Matrizen mit den gleichen relativen Häufigkeiten, sie sind also nicht zu unterscheiden.

Die Bedingungen 1. und 2. werden auch Kontrast genannt. Die 3. Bedingung nennt man Sicherheit. Sie besagt, dass man beim Betrachten von weniger als k Folien keine Hinweise auf die geheime Botschaft bekommt. Es werden mindestens k Folien gebraucht.

2.3 Matrizen für ein 2 aus 2-Schema:

Als Matrizen für dieses Verfahren wären folgende ausreichend:

C_0 = {alle Spalten-Permutationen von: $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ }

C_1 = {alle Spalten-Permutationen von: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ }

Anschaulich kann man sich vorstellen, dass man „von oben“ auf die Matrizen schaut. In der Spalte, wo nur Nullen zu sehen sind, ist die Farbe Weiß bzw. transparent. Wo mindestens eine Eins steht, ist die Farbe Schwarz.
Man erkennt leicht, dass alle $S_0 \in C_0$ ein 50%iges Grau liefern (Die Hälfte der Unterpunkte ist schwarz, die andere Hälfte ist weiß bzw. transparent) und alle $S_1 \in C_1$ ein 100%iges Grau, also Schwarz (Alle Unterpunkte und damit der alle Bildpunkte sind schwarz).
In der Praxis ergibt sich das Problem, dass dabei nur 2 Unterpunkte für jeden Bildpunkt erzeugt werden. Dadurch wird das Bild verzerrt. Man kann aber folgende Matrizen verwenden, welche 4 Unterpunkte für jeden Bildpunkt erzeugen:

C_0 = {alle Spalten-Permutationen von: $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$ }

C_1 = {alle Spalten-Permutationen von: $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ }

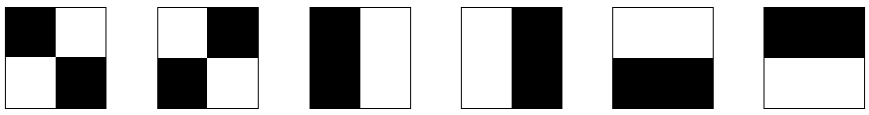

Abbildung 2: Die zu obigen Matrizen passenden Shares.

Eine Alternative zum Verdoppeln der Anzahl der Unterpunkte ist das Verwenden von nicht quadratischen Unterpunkten mit einem Seitenverhältnis von 2:1. Dann erscheint die entschlüsselte Botschaft mit den ursprünglichen Proportionen.

2.4 Ähnlichkeiten zum One-Time-Pad:

Das 2 aus 2-Schema entspricht im Prinzip dem One-Time-Pad. Ein Bit des Schlüssels bzw. der geheimen Botschaft beim One-Time-Pad entspricht gerade einem *Share* des 2 aus 2-Schemas. Ist man im Besitz nur einer der Informationen kann man keine Aussage über den Klartext treffen da man jedes Bit / jedes *Share* mit gleicher Wahrscheinlichkeit erhält, unabhängig vom Klartext.
Allerdings handelt es sich bei der zugrunde liegenden Struktur des 2 aus 2-Schemas nicht um eine Gruppe ($\{0, 1\}, \otimes$) wie beim One-Time-Pad sondern nur um eine Halbgruppe ($\{0, 1\}, \vee$), da zur „1“ kein inverses Element bezüglich „$\vee$“ existiert. Deshalb kann ein weißer Bildpunkt des Originalbildes nicht wieder in einen komplett weißen Bildpunkt zurück verwandelt werden. Ein weißer Bildpunkt müsste hierfür durch zwei komplett weiße *Shares* kodiert werden, ein schwarzer durch mindestens ein nicht weißen. Dadurch würde der Betrachter eines *Shares* bereits Informationen über die geheime Nachricht erhalten.

2.5 Entschlüsseln:

Zum Entschlüsseln werden die Folien mit dem geheimen Schlüssel und der verschlüsselten Botschaft übereinander gelegt. Im Original schwarze Punkte bleiben schwarz, da alle möglichen Unterpunkte übereinander gelegt Schwarz ergeben. Bei einem weißen Punkt im Original ist allerdings die Hälfte der Unterpunkte schwarz. Die Farbe Weiß im Original wird zu einem 50%-igem Grau. Das Original bleibt erkennbar, erleidet aber einen Kontrastverlust.

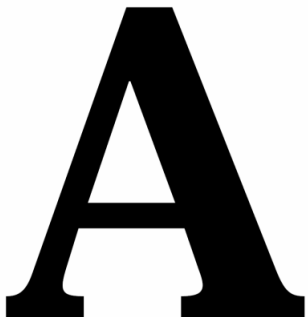

Abbildung 3: Das Original.

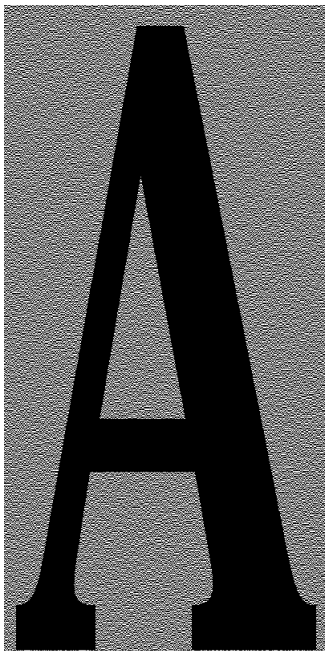

Abbildung 4: Beide Folien eines 2 aus 2-Schemas übereinander gelegt. Man beachte das falsche Seitenverhältnis (VslCrypt).

Das Beispiel verdeutlicht es: Aus dem Original (Abbildung 3) wurde mittels dem Programm VslCrypt ein 2 aus 2-Schema generiert. Jede Folie für sich alleine enthält nur ein Rauschen. Beide Folien zusammen ergeben wieder das Original. Allerdings ist das Bild verzerrt (Abbildung 4). Man erkennt aber gut, dass das Weiß im Original einem Grau gewichen ist. Dieses Grau besteht aus weißen und schwarzen Bildpunkten, wie man auf der Vergrößerung (Abbildung 5) sieht.

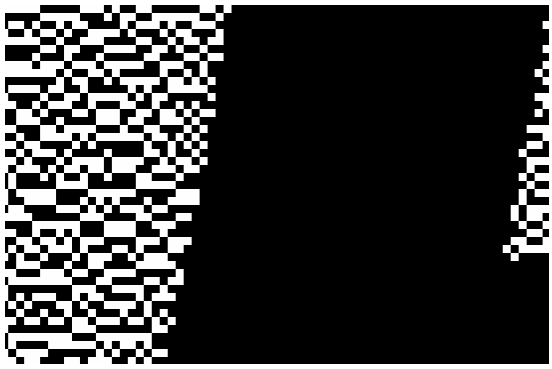

Abbildung 5: Ein Ausschnitt aus Abbildung 4 stark vergrößert.

3. Lösungen für kleine *n* und *k*:

3.1 Das 2 aus *n*-Schema:

Eine Lösung für das 2 aus *n*-Schema stellen folgende Mengen C_0 und C_1 dar:

C_0 = {alle Spalten-Permutationen von: $\begin{pmatrix} 100...0 \\ 100...0 \\ ... \\ 100...0 \end{pmatrix}$ }

C_1 = {alle Spalten-Permutationen von: $\begin{pmatrix} 100...0 \\ 010...0 \\ ... \\ 000...1 \end{pmatrix}$ }

Die Kombination zweier beliebiger *Shares* aus einer Matrix $S_0 \in C_0$ hat ein Hamminggewicht von 1, bei zwei beliebigen schwarze *Shares* aus einer Matrix $S_1 \in C_1$ ergibt sich ein Hamminggewicht von 2. Das Hamminggewicht einer Kombination von *Shares* ist umgekehrt proportional zur Helligkeit der Bildpunkte.

3.2 Das 3 aus 3-Schema:

Das 3 aus 3-Schema kann durch folgende Matrizen gelöst werden:

C_0 = {alle Spalten-Permutationen von: $\begin{pmatrix} 0011 \\ 0101 \\ 0110 \end{pmatrix}$ }

C_1 = {alle Spalten-Permutationen von: $\begin{pmatrix} 1100 \\ 1010 \\ 1001 \end{pmatrix}$ }

Die sechs *Shares* der Zeilen aus C_0 und C_1 entsprechen genau den sechs *Shares* aus Abbildung 2. Jede Matrix enthält jeweils ein horizontales, ein vertikales und ein diagonales *Share*. Eine Zeile einer Matrix repräsentiert je ein weißen und ein schwarzen Unterpunkt und enthält genau zwei schwarze Unterpunkte. Zwei beliebige *Shares* einer Matrix ergeben immer genau drei schwarze Unterpunkte. Es kann also anhand des Grauwertes eines Bildpunktes nicht zwischen einer Matrix aus C_0 oder C_1 entschieden werden wenn man im Besitz nur zweier Folien ist. Erst das Übereinander legen von drei Folien zeigt, das ein „weißer" Bildpunkt zu 75% schwarz ist, während ein schwarzer Bildpunkt komplett schwarz ist.

4. Das *n* aus *n*-Schema:

Allgemein kann man ein n aus n-Schema nach folgendem Prinzip konstruieren:
Für die weißen Bildpunkte gilt: S_0 ist eine $n \times 2^{n-1}$-Matrix aus C_0, welche alle 2^{n-1} Spalten mit einer geraden Anzahl von Einsen enthält. Für die schwarzen Bildpunkte gilt: S_1 ist eine $n \times 2^{n-1}$-Matrix aus C_1, welche alle 2^{n-1} Spalten mit einer ungeraden Anzahl von Einsen enthält. Dann ist das angegebene Schema ein n aus n-Schema mit

$$m = 2^{n-1},\ \alpha = 1 / 2^{n-1} \text{ und } r = 2^{n-1}!.$$

Da S_0 eine Spalte enthält, die nur aus Nullen besteht, ist das Hamminggewicht des ODER-Vektors $H(V)$ bei einem weißen Bildpunkt geringer als bei einem schwarzen Bildpunkt (Kontrast).
Beschränkt man die Matrizen S_0 und S_1 auf beliebige n-1 Spalten, so erhält man eine Matrix, die jeden möglichen Spaltenvektor V genau einmal enthält. Daher kann man die Mengen C_0 und C_1 anhand der Matrizen nicht unterscheiden (Sicherheit).

Beispiel eines 4 aus 4-Schemas:
Sei $n = 4$, $S_0 \in C_0$ und $S_1 \in C_1$ wie oben. Dann gilt:

$m = 2^{n-1} = 2^{4-1} = 8$,
$\alpha = 1 / 2^{n-1} = 1 / 2^{4-1} = 1 / 8 = 0{,}125$,
$r = 2^{n-1}! = 2^{4-1}! = 40320$.
Weiterhin gilt für S_0: $H(V) \leq d - \alpha * m.$; $d = 1 \ldots m$
$7 \leq 7.$
Weiterhin gilt für S_1: $H(V) \geq d.$; $d = 1 \ldots m$
$8 \geq 8.$

D. h., es gibt einen visuell erkennbaren Unterschied zwischen schwarzen und weißen Bildpunkten auf den Folien ($7 < 8$).

C_0 = {alle Spalten-Permutationen von: $\begin{pmatrix} 01001011 \\ 01100101 \\ 00111001 \\ 00010111 \end{pmatrix}$ }

C_1 = {alle Spalten-Permutationen von: $\begin{pmatrix} 00011110 \\ 00101011 \\ 01000111 \\ 10001101 \end{pmatrix}$ }

Man kann nun noch zeigen, dass α im Verhältnis zu n exponentiell klein wird, genauer $\alpha \leq 1 / 2^{n-1}$. Es folgt auch, dass $m \geq 1 / 2^{n-1}$. Näheres dazu in der Veröffentlichung von Moni Naor und Adi Shamir.

5. Das *k* aus *n*-Schema:

Das ursprüngliche Modell ist ein 2 aus 2-Schema. Es wurde später von beiden Autoren zu einem *k* aus *n*-Schema weiterentwickelt. Es sind beliebige Varianten mit *k* aus *n* Folien möglich, d.h. es werden *k* der *n* Folien benötigt, um die Information zurückzuerhalten.

6. Erweiterungen:

- Man kann für die geheime Botschaft Graustufen benutzen, anstatt nur Schwarz und Weiß. Der Grauwert der Bildpunkte kann dann zwischen 50% und 100% variiert werden, indem man anstatt rechteckiger Bildpunkte Kreise nimmt. Diese sind je zur Hälfte schwarz und weiß (transparent). In einem 2 aus 2-Schema stehen die Kreise in einem beliebigen Winkel. Durch „Drehen" der Kreise in den anderen *Shares* verkleinert man den transparenten Bereich. So kann man die Helligkeit des Bildpunktes übergangslos zwischen 50% und 100% variieren.

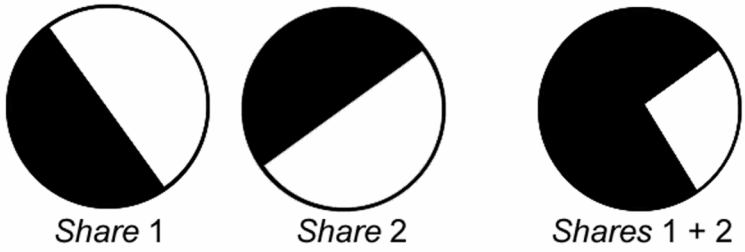

Abbildung 6: Beispiel für ein 2 aus 2-Schema mit Kreisen.

- Zugriffsstrukturen: Sei $T = \{1 \ldots n\}$ die Menge der Teilnehmer, die sich ein Geheimnis teilen wollen. Eine Zugriffsstruktur ist eine Teilmenge $\Gamma \subseteq 2^T$. Eine Gruppe von Teilnehmern am *Secret Sharing* kann die geheime Botschaft nur dann entschlüsseln, wenn sie oder eine Teilmenge von ihr in Γ enthalten ist. Ein Beispiel für $n = 4$ ist $\Gamma = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3, 4\}\}$.

- Eine weitere mögliche Erweiterung besteht darin, die geheime Botschaft nicht in rein zufällig erzeugte Bilder zu verstecken, sondern in Bildern mit erkennbarem Inhalt. Dieser hat allerdings nichts mit der geheimen Botschaft zu tun. Dadurch erregt man weniger schnell den Verdacht, etwas zu verbergen. (**E**xtended **V**isual **C**ryptography **S**cheme: **EVCS**).

- Mehr Farben benutzen: Man kann z. B. zwei verschiedene Farben plus einer völlig transparenten benutzen. Durch die Farbmischung beim Übereinander legen der Folien ergeben sich verschiedene Farbabstufungen. Wenn z. B. ein roter Punkt und viele transparente Punkte sich addieren, ergibt sich ein hellerer Ton, als wenn alle Punkte rot wären. Das erhöht die Erkennbarkeit des Bildes.

7. Zusammenfassung:

- ✓ Simples System, bedarf keiner speziellen Kenntnisse oder Rechenpower. Nur das menschliche Auge dient der Entschlüsselung.
- ✓ Schlüssel und geheime Botschaft können z. B. per Fax / E-Mail oder Post verschickt werden.
- ✓ Aufteilung einer geheimen Botschaft in Bildpunkte und weitere Unterpunkte, welche per Zufall entweder schwarz oder weiß eingefärbt werden.
- ✓ Das Verfahren ist absolut sicher, es entsteht auf jeder Folie ein dem Rauschen ähnliches Muster.
- ✓ *k* aus *n*-Schema: Mindestens *k* von *n* Personen müssen kooperieren, damit die geheime Botschaft entschlüsselt werden kann.
- ✓ Kontrast- und Sicherheitsbedingung müssen erfüllt sein.
- ✓ Erweiterungen (Kreise, Farben Zugriffsstrukturen, EVCS) möglich.

8. Literatur und Links:

1. Homepage von Moni Naor: http://www.wisdom.weizmann.ac.il/~naor/

   - Moni Naor and Adi Shamir, ***Visual Cryptography***, *EUROCRYPT ´94*.
   - Moni Naor and Adi Shamir, ***Visual Cryptography II***, Cambridge Workshop on Protocols, 1996.
   - Moni Naor and Benny Pinkas, ***Visual Authentication***, *CRYPTO ´97*.

2. Homepage von Douglas R. Stinson:
   http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html

   - Douglas R. Stinson, ***Visual Cryptography***, 1997.
   - Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis und Douglas R. Stinson, ***Constructions and Bounds for Visual Cryptography***, *ICALP ´96*.
   - Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis und Douglas R. Stinson, ***Visual Cryptography for general Access Structures***, Information and Computation 1996.
   - Carlo Blundo, Alfredo De Santis und Douglas R. Stinson, ***On the Contrast in Visual Cryptography Schemes***, Information and Computation 1996.
   - Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis und Douglas R. Stinson, ***Extended Schemes for Visual Cryptography***, 1996.

3. Homepage von Klaus Reinhardt mit den Java-Programmen von Holger Schmid:
   http://www-fs.informatik.uni-tuebingen.de/~reinhard/krypto/Visual/Visual_Applet_d.html
4. Markus Maucher, ***Visuelle Kryptographie,*** 10. Februar 2000.
   http://theorie.informatik.uni-ulm.de/Lehre/WS9900/sichere-tel/maucher.ps
5. Matthias Baumgart (matthias.baumgart@math.uni-giessen.de) und Markus Hoek (markus.hoek@math.uni-giessen.de) (Folienprgramm **Vslcryp**): http://www.uni-giessen.de/~gc95/